EXHIBIT A

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

KENSANDRA SMITH and **MARY ELLEN NILLES**, Individually and on behalf of all others similarly situated,

Plaintiffs,

v.

LOYOLA UNIVERSITY MEDICAL CENTER,

Defendant.

CAUSE NO: 2023CH08410

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Kensandra Smith and Mary Ellen Nilles, individually and on behalf of all others similarly situated (hereinafter "Plaintiffs"), bring this Class Action Complaint against Defendant Loyola University Medical Center ("LUMC" or "Defendant"), and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this action to address Defendant's transmission and disclosure of Plaintiffs' and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information" or "PII and PHI") to Meta Platforms, Inc. d/b/a Meta ("Facebook") and/or Google LLC d/b/a Google ("Google") via tracking pixels ("Tracking Pixels" or "Pixel") installed on Defendant's website.

2. Plaintiffs' and Class Members' Private Information was unlawfully intercepted, and, upon information and good faith belief, the information transmitted to and received by third-parties included the following: IP addresses and cookie identifiers; dates, times, and/or locations

of scheduled appointments; proximity to LUMC; information about specific providers; types of appointments or procedures; the buttons, links, pages, and tabs that patients click and view; insurance information; and, contents of patients' searches for specific providers, conditions, or treatments on Defendant's Website.

3. Information about a person's physical and mental health is among the most confidential and sensitive information in our society, and the mishandling of medical information can have serious consequences, including discrimination in the workplace or denial of insurance coverage. If people do not trust that their medical information will be kept private, they may be less likely to seek medical treatment, which can lead to more serious health problems down the road. In addition, protecting medical information and making sure it is kept confidential and not disclosed to anyone other than the person's medical provider is necessary to maintain public trust in the healthcare system as a whole.

4. Recognizing these facts, and in order to implement requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the United States Department of Health and Human Services ("HHS") has established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") governing how healthcare providers must safeguard and protect Private Information. Under the HIPAA Privacy Rule, **no** healthcare provider can disclose a person's personally identifiable protected health information to a third party without express written authorization.

5. LUMC is a healthcare system headquartered in Chicago, Illinois that consists of hospitals in Chicago, Melrose Park, and Berwyn; 15 primary and specialty care locations throughout the Chicago-area; a large network of clinics throughout Cook, Will, and DuPage

counties; and approximately 1,350 primary and specialty care providers.[1] In spite of its unique position as a massive and trusted healthcare provider, LUMC knowingly configured and implemented a software device known as a tracking pixel to collect and transmit information from loyolamedicine.org (the "Website") to third parties, including confidential patient searches through the "Find a Doctor" tab on the Website and, upon information and good faith belief, information communicated in the sensitive and presumptively confidential myLoyola patient portal (the "Disclosure").[2]

6. Plaintiffs and Class Members are individuals who are seeking or have sought medical services and/or treatment from Defendant. Defendant advertises its online services on its Online Platforms to assist patients with their medical care, and Defendant encouraged its patients to use its Online Platforms for booking medical appointments and procedures; locating treatment facilities; searching for physicians and information about specific medical conditions, treatment options, and services; communicating medical symptoms; signing up for events and classes; and more.

7. Plaintiffs and other Class Members who used Defendant's Online Platforms thought they were communicating only with their trusted healthcare provider. Unbeknownst to Plaintiffs and Class Members, however, Defendant has embedded the Facebook Tracking Pixel (the "Tracking Pixel" or "Pixel"), on its Online Platforms, surreptitiously forcing Plaintiffs and Class Members to transmit to Facebook and other third parties every click, keystroke, and intimate detail about their medical treatment. Operating as designed and as implemented by Defendant, the

[1] *About Loyola*, LOYOLA MEDICINE, https://www.loyolamedicine.org/about-us/ (last visited Aug. 22, 2023); *Find a Doctor*, LOYOLA MEDICINE, https://www.loyolamedicine.org/find-a-doctor/ (last visited Aug. 22, 2023).

[2] Defendant's Website and myLoyola patient portal are collectively referred to as Defendant's "Online Platforms".

Pixel allows the Private Information that Plaintiffs and Class Members submit to Defendant to be unlawfully disclosed to Facebook and other third parties alongside the individual's IP address and unique and persistent Facebook ID ("FID").[3]

8. A pixel is a piece of code that "tracks the people and [the] type of actions they take"[4] as they interact with a website, including how long a person spends on a particular web page, which buttons the person clicks, which pages they view, and the text or phrases they type into various portions of the website (such as a general search bar, chat feature, or text box), among other things.

9. The user's web browser executes the Pixel via instructions within the webpage to communicate certain information based on parameters selected by the website's owner. The Tracking Pixel is thus customizable and programmable, meaning that the website owner controls which of its pages contain the Pixel and which events are tracked and transmitted to Facebook and other third-party tracking technology vendors. By installing the Tracking Pixel on its Online Platforms, Defendant effectively planted a bug on Plaintiff's and Class Members' web browsers and compelled them to disclose their communications with Defendant to Facebook and other likely third parties.

[3] The Pixel forces the website user to share the user's FID for easy tracking via the "cookie" Facebook stores every time someone accesses their Facebook account from the same web browser. "Cookies are small files of information that a web server generates and sends to a web browser." *What are cookies?*, CLOUDFLARE, https://www.cloudflare.com/learning/privacy/what-are-cookies/ (last visited Aug. 21, 2023). "Cookies help inform websites about the user, enabling the websites to personalize the user experience." *Id.*

[4] *Regargeting*, META, https://www.facebook.com/business/goals/retargeting (last visited Aug. 21, 2023).

10. In addition to the Tracking Pixel, Defendant also likely installed and implemented Facebook's Conversions Application Programming Interface ("CAPI") on its network servers.[5]

11. Unlike the Tracking Pixel, which co-opts a website user's browser and forces it to transmit information to Facebook in addition to the website owner, CAPI does not cause the user's browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website interaction, including Private Information, records and stores that information on the website owner's servers, and then transmits the data to Facebook from the website owner's servers.[6] Indeed, Facebook markets CAPI as a "better measure [of] ad performance and attribution across your customer's full journey, from discovery to conversion. This helps you better understand how digital advertising impacts both online and offline results."[7]

12. Because CAPI is located on the website owner's servers and is not a bug planted onto the website user's browser, it allows website owners like Defendant to circumvent any ad blockers or other denials of consent by the website user that would prevent the Pixel from sending website users' Private Information to Facebook directly.

---

[5] "CAPI works with your Facebook pixel to help improve the performance and measurement of your Facebook ad campaigns." *See* Samir ElKamouny, *How to Implement Facebook Conversions API (In Shopify)*, FETCH&FUNNEL, https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/ (last visited Aug. 21, 2023).

[6] *What is the Facebook Conversion SPI and How to Use It*, REVEALBOT BLOG, https://revealbot.com/blog/facebook-conversions-api/ (last visited Aug. 21, 2023). "Server events are linked to a dataset ID and are processed like events sent via the Meta Pixel . . . . This means that server events may be used in measurement, reporting, or optimization in a similar way as other connection channels." *Conversions API*, META FOR DEVELOPERS, https://developers.facebook.com/docs/marketing-api/conversions-api/ (last visited Aug. 21, 2023).

[7] *About Conversions API*, META, https://www.facebook.com/business/help/2041148702652965?id=818859032317965 (last visited Aug. 21, 2023).

13. Defendant utilized the Tracking Pixel and CAPI data for marketing purposes in an effort to bolster its profits. The Tracking Pixel and CAPI are routinely used to target specific customers by utilizing data to build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiffs' and Class Members' Private Information to create targeted advertisements based on the medical conditions and other information disclosed to Defendant.

14. The information that Defendant's Tracking Pixel and CAPI sent to Facebook and other third parties included the Private Information that Plaintiffs and Class Members submitted to Defendant's Online Platforms, including for example, the type of medical treatment sought, the individual's particular health condition, and the fact that the individual attempted to or did book a medical appointment.

15. Such information allows a third-party (e.g., Facebook) to know that a specific patient was seeking confidential medical care. Facebook, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who geotarget Plaintiffs' and Class Members' Facebook pages based on communications obtained via the Tracking Pixel and CAPI. Facebook and any third-party purchasers of Plaintiffs' and Class Members' Private Information also could reasonably infer from the data that a specific patient was being treated for a specific type of medical condition, such as cancer, pregnancy, dementia, or HIV.

16. The third party, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who online target[8] Plaintiffs and Class Members based on communications obtained via the Tracking Pixel.

[8] "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." *See A Guide to Online Targeting – Which Works For Your Business*, DIGITAL MARKETING GROUP, https://digitalmarketinggroup.com/a-guide-to-online-targeting-which-works-for-your-business/ (last visited Aug. 21, 2023).

17. Healthcare patients simply do not anticipate that their trusted healthcare provider will send personal health information or confidential medical information collected via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy violations in pursuit of ever-increasing advertising revenue—without the patient's consent. Neither Plaintiffs nor any other Class Member signed a written authorization permitting Defendant to send their Private Information to Facebook.

18. Despite willfully and intentionally incorporating the Tracking Pixel and CAPI into its Online Platforms and servers, Defendant has never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications and Private Information with Facebook and other likely third parties. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted to unauthorized third parties as they communicated with their healthcare provider via the Online Platforms, or stored on Defendant's servers to be later transmitted to Facebook so it could be used for targeted advertising and marketing purposes.[9]

19. Defendant further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchanged with Defendant.

[9] In contrast to Defendant, in recent months several medical providers which have installed the Facebook Pixel on their web properties have provided their patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, CEREBRAL, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf (last visited Aug. 15, 2023); *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies*, FIERCE HEALTHCARE (Oct. 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health 1.36 Million Patients About Unauthorized Disclosure of PHI via Meta Pixel Code on Patient Portal*, THE HIPAA JOURNAL (Aug. 16, 2022), https://www.hipaajournal.com/novant-health-notifies-patients-about-unauthorized-disclosure-of-phi-via-meta-pixel-code-on-patient-portal/.

20. Defendant owed common law, statutory, and regulatory duties to keep Plaintiffs' and Class Members' communications and medical information safe, secure, and confidential.

21. The disclosure of Plaintiffs' and Class Members' Private Information via the Pixel contravenes the letter and spirit of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). As part of HIPAA, the United States Department of Health and Human Services ("HHS") established "Standards for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule") which governs how health care providers must safeguard and protect Private Information.

22. Simply put, further to the HIPAA Privacy Rule, covered entities such as Defendant are ***not*** permitted to use tracking technology tools (like pixels) in a way that exposes patients' Private Information to any third-party without express and informed consent from each patient.

23. Lest there be any doubt of the illegal nature of Defendant's practice, the Office for Civil Rights (OCR) at HHS has made clear, in a recent bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the unlawful transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[10]

24. The HHS Bulletin does not change any existing rule or impose any new obligation on HIPAA-covered entities. Instead, it reminds these entities of their long-standing obligations by

[10] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Aug. 21, 2023) (emphasis added).

referring to guidance and rules that have been in place for decades. *Id.* ("it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology").

25. Upon information and good faith belief, Defendant utilized the Pixel data to improve and to save costs on its marketing campaigns, improve its data analytics, and attract new patients.

26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and to safeguard that information from unauthorized disclosure.

27. However, as set forth more fully below, Defendant failed in its obligations and promises by using Tracking Pixels while knowing that doing so would result in the transmission and disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties with a long history of privacy violations and misconduct—i.e. Facebook.

28. Plaintiffs and Class Members Private Information can—and likely will—be further exploited and disseminated for retargeting, marketing, or insurance companies utilizing the information to set insurance rates.

29. Defendant breached its statutory and common law obligations to Plaintiffs and Class Members by, *inter alia*: (i) failing to adequately review its marketing programs and web based technology to ensure the Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) aiding, agreeing, and conspiring with third-parties to intercept communications sent and received by Plaintiffs and Class Members; (iv) failing to obtain the written consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, Google, or others; (v) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Pixels;

(vi) failing to warn Plaintiffs and Class Members; and (vii) otherwise failing to design and monitor its Online Platforms to maintain the confidentiality and integrity of patient Private Information.

30. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Tracking Pixel, (iii) loss of benefit of the bargain, (iv) diminution or deprivation of value of the Private Information, (v) statutory damages, and (vi) the continued and ongoing risk of exposure of their Private Information.

31. Plaintiffs seek to remedy these harms and brings causes of action for (I) Negligence, (II) Negligence Per Se, (III) Invasion of Privacy, (IV) Breach of Implied Contract, (V) Unjust Enrichment, (VI) Breach of Implied Duty of Confidentiality, (VII) Violation of Illinois Consumer Fraud and Deceptive Business Practices Act, and (VIII) Violation of Illinois Eavesdropping Statute.

THE PARTIES

32. Plaintiff Kensandra Smith is a natural person, resident, and a citizen of Illinois. She has no intention of moving to a different state in the immediate future. Plaintiff is a former patient of Defendant.

33. Plaintiff Mary Ellen Nilles is a natural person, resident, and citizen of Illinois. She has no intention of moving to a different state in the immediate future. Plaintiff is a current patient of Defendant.

34. Defendant Loyola University Medical Center is an Illinois non-profit corporation with its principal place of business at 2160 South First Avenue, Maywood, Illinois 60153. Loyola University Medical Center can be served with process in this matter through its registered agent

for service, C T Corporation System, at 208 South Lasalle Street, Suite 814, Chicago, Illinois 60604.

JURISDICTION AND VENUE

35. This Court has jurisdiction over Defendant by virtue of 735 ILCS 5/2-209 because LUMC operates and provides services within the state of Illinois, committed statutory violations and tortious acts in the state of Illinois, and is organized under the laws of the state of Illinois.

36. Venue is proper in this Court, as a substantial part of the events giving rise to the claims emanated from activities within this County, and LUMC conducts substantial business in this County.

COMMON FACTUAL ALLEGATIONS

A. Background

37. LUMC is one of the largest healthcare providers in the Chicago metropolitan area and serves many of its patients via its Online Platforms, which it encourages patients to use for searching for providers, scheduling appointments and/or procedures, communicating with their healthcare providers, reviewing their medical histories, and communicating other information related to their treatment and status as a patient.

38. Defendant utilizes its Online Platforms to connect Plaintiffs and Class Members to Defendant's digital healthcare services with the goal of increasing profitability.

39. In furtherance of that goal, and to increase the success of its advertising and marketing, Defendant purposely installed the Tracking Pixels on its Online Platforms to advertise its services to Plaintiffs and Class Members. In doing so, Defendant surreptitiously tracked, recorded, transmitted, and disseminated its patients' private and protected communications with

Facebook and other third parties, including communications that contain Plaintiffs' and Class Members' Private Information.

40. While seeking and using Defendant's services as a medical provider via its Online Platforms, Plaintiffs' and Class Members' Private Information was intercepted by third parties via the Tracking Pixels, and it was also transmitted to third parties by Defendant via first-party cookies and Conversion API tools.

41. Plaintiffs and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook, Google, or other third parties, or that Defendant was tracking their every communication and disclosing the same to third parties when they entered highly sensitive information on Defendant's Online Platforms.

42. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information.

43. Upon information and good faith belief, Defendant intercepted and disclosed Plaintiffs' and Class Members': (1) status as medical patients; (2) communications with Defendant through its Online Platforms; and (3) information about their medical appointments, location of treatments, specific medical providers, specific medical conditions and treatments, and related information.

44. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Tracking Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook, Google, and/or other unauthorized third-parties; and (3) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

45. To better understand Defendant's unlawful data-sharing practices, a brief discussion of basic web design and tracking tools follows:

i. Facebook's Business Tools and the Pixel

46. Facebook operates the world's largest social media company, which generated $117 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.[11]

47. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses.

48. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.

49. Facebook then sells advertising space by highlighting its ability to target users.[12] Facebook can target users so effectively because it surveils user activity both on and off its site.[13] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[14] Facebook compiles this information into a

[11] *Meta Reports Fourth Quarter and Full Year 2021 Results*, META INVESTOR RELATIONS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Aug. 22, 2022).

[12] *Why Advertise on Facebook, Instagram, and other Meta technologies*, META, https://www.facebook.com/business/help/205029060038706 (last visited Aug. 21, 2023).

[13] *About Meta Pixel*, META, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Aug. 21, 2023).

[14] *Audience ad targeting*, META, https://www.facebook.com/business/ads/ad-targeting (last visited Aug. 21, 2023).

generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[15]

50. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

51. Advertisers can also build "Custom Audiences."[16] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[17] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[18] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," including the Tracking Pixel.[19]

---

[15] *Core-Audiences*, META, https://www.facebook.com/business/news/Core-Audiences (last visited Aug. 21, 2023).

[16] *About custom audiences*, META, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Aug. 21, 2023).

[17] *Audience ad targeting*, *supra* note 13.

[18] *About lookalike audiences*, META, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Aug. 21, 2023).

[19] *Create a customer list custom audience*, META, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Aug. 21, 2023); *Create a website custom audience*, META, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Aug. 21, 2023).

52. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[20] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept, collect, view, and use user activity on those platforms.

53. In conjunction with its advertising business, Facebook encourages and promotes entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify, target, and market products and services to individuals.

54. Facebook's Business Tools, including the Tracking Pixel and Conversions API, are bits of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby enabling the interception and collection of user activity on those platforms.

55. The Business Tools are automatically configured to capture "Standard Events" such as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"), as well as metadata, button clicks, and other information.[21] Businesses that want to target

[20] *The Meta Business Tools*, META, https://www.facebook.com/help/331509497253087 (last visited Aug. 21, 2023).

[21] *Specifications for Meta Pixel Standard Events*, META, https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Aug. 21, 2023); *see Facebook Pixel, Accurate Event Tracking, Advanced*, META, https://developers.facebook.com/docs/meta-pixel/advanced (last visited Aug. 21, 2023); *see also Best Practices for Meta Pixel Setup*, META, https://www.facebook.com/business/help/218844828315224?id=120537668220832142 (last visited Aug. 21, 2023); *App Events API*, META, https://developers. facebook.com/docs/marketing-api/app-event-api/ (last visited Aug. 21, 2023).

customers and advertise their services, such as Defendant, can track other user actions and can create their own tracking parameters by building a "custom event."[22]

56. One such Business Tool is the Tracking Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their websites. As the name implies, the Tracking Pixel "tracks the people and the types of actions they take."[23] When a user accesses a website hosting the Tracking Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers at certain times during interaction with the webpage. This second, secret transmission contains the original request sent to the host website, along with additional data that the Tracking Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Online Platforms—Defendant's own code, and Facebook's embedded code.

57. Accordingly, during the same transmissions, the Online Platforms routinely provide Facebook with Defendant's patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant's Online Platforms, including not only their medical searches, treatment requests, and the webpages they view, but also their home address, zip code, or phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[24] Plaintiffs' and

---

[22] *About standard and custom website events*, META, https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (last visited Aug. 21, 2023); *see also App Events API*, *supra* note 20.

[23] *Retargeting*, *supra* note 3.

[24] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Aug. 21, 2023).

Class Members identities can be easily determined based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

58. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the website visitor is also a Facebook user, the information collected via the Tracking Pixel is associated with the user's Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

59. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

60. Notably, this transmission only occurs on webpages that contain a Pixel. A website owner can configure its website to use the Pixel on certain webpages that don't implicate privacy and disable it on pages that do implicate patient privacy. Thus, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook or other third parties via the Tracking Pixels but for Defendant's decisions to install the Pixel on its Online Platforms and specifically on webpages that solicit and receive Private Information.

61. Similarly, Plaintiffs' and Class Members' Private Information would not have been disclosed to Facebook via Conversions API but for Defendant's decision to install and implement that tool on its servers.

62. By installing and implementing both tools, Defendant caused Plaintiffs' and Class Members' communications to be intercepted and transmitted from Plaintiffs' and Class Members'

browsers directly to Facebook via the Pixel, or to be recorded on Defendant's servers and then transferred to Facebook via Conversions API.[25]

ii. Defendant's method of transmitting Plaintiff's and Class Members' Private Information via the Tracking Pixel and/or Conversion API i.e., the Interplay between HTTP Requests and Responses, Source Code, and the Pixel

63. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as a computer, tablet, or smart phone) accesses web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

64. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

65. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.

[25] Facebook assigns a unique "event_id" parameter to each separate communication with a website and then duplicates the data based on the event_id so that the same event tracked by the Pixel and recorded by the CAPI are not reported as two separate events. *Set Up Conversions API for Server-Side Tagging in Google Tag Manager*, META, https://www.facebook.com/business/help/702509907046774 (last visited Aug. 21, 2023).

- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data.

66. When an individual visits Defendant's Online Platforms, their web browser sends an HTTP Request to Defendant's servers that essentially asks Defendant's Online Platforms to retrieve certain information (such as Defendant's "Find a Doctor" page). Defendant's servers send the HTTP Response, which contains the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Online Platforms.

67. Every website is comprised of Markup and "Source Code." Source Code is a set of instructions invisible to the website's visitor that commands the visitor's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

68. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to Defendant's server, Defendant's server sends an HTTP Response including the Markup that

displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is in essence handing patients a tapped phone, and once the webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

69. Separate from the Pixel, Facebook and other website owners can place third-party cookies in the web browsers of users logged into their websites or services. These cookies can uniquely identify the user so the cookie owner can track the user as he or she moves around the internet—whether on the cookie owner's website or not. Facebook uses this type of third-party cookie when Facebook account holders use the Facebook app or website. As a result, when a Facebook account holder uses Defendant's Online Platforms, a unique id is sent to Facebook along with the intercepted communication that allows Facebook to identify the patient associated with the Private Information it has intercepted.

70. Furthermore, if the patient is also a Facebook user, the information Facebook receives is linked to the patient's Facebook profile (via their FID), which includes other identifying information.

71. Defendant intentionally configured the Pixels installed on its Online Platforms to capture both the "characteristics" of individual patients' communications with the Defendant's Website (*i.e.,* their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the buttons, links, pages, and tabs they click and view).

72. As an example, anyone who visits LUMC's Website, *https://www.loyolamedicine.org/*, and clicks on the "Find a Service of Specialty" tab is presented

with a search bar and a list of approximately 79 links to pages with information on specific conditions, treatments, services, and locations, ranging from "Adolescent Medicine" to "Wound Center." Someone who clicks on the "Cancer" button is directed to a page, *https://www.loyolamedicine.org/find-a-condition-or-service/cancer/*, which includes buttons and links that allow patients to schedule appointments and provide information about specific conditions, treatment options, services, locations, doctors, clinical trials, each with a separate link. Selecting any of these links, like "Breast Cancer," directs them to a new page, *https://www.loyolamedicine.org/find-a-condition-or-service/cancer/cancer-conditions/breast-cancer/*, providing more information about breast cancer, treatment options, and services, many of which have additional links and associated pages.

73. The Tracking Pixel intercepts the "characteristics" and "content" of all these communications with the LUMC Website, and automatically transmits this data to Facebook. Thus, by receiving the contents of these communications, Facebook will know the exact webpages that a specific patient has viewed and buttons clicked on, which relates to the patient's past, present, or future health conditions (*i.e.*, the patient's individually-identifiable patient health information).

74. As another example, when a patient visits the *https://www.loyolamedicine.org/* homepage, navigates to the search bar, and types in specific search terms, that information is shared with Facebook through the Pixel in the form of full string URLs. Thus, on information and good faith belief, if a patient types in "Crohn's Disease" into the search bar, when the webpage loads into the patient's browser, the Pixel code is triggered which secretly sends an HTTP Request to Facebook including the patient's FID and the URL, informing Facebook that the user is searching

for information on Crohn's Disease by transmitting the following URL to Facebook: "https://www.loyolamedicine.org/site-search/?q=Crohn%27s%20Disease."

75. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. To counteract this, third parties bent on gathering data and Private Information implement workarounds that are difficult to detect or evade. Facebook's workaround, for example, is its Conversions API tool, which is particularly effective because the data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the information travels directly from Defendant's server to Facebook's server.

76. Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]."[26] Thus, the communications between patients and Defendant, which are necessary to use Defendant's Online Platforms, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

77. While there is no way to confirm with certainty that a website owner is using Conversions API without accessing the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[27] Thus, it is reasonable to infer that Facebook's customers who

[26] *Prepare Your Business to Use the Conversions API*, META, https://www.facebook.com/business/help/1295064530841207?id=818859032317965 (last visited Aug. 21, 2023).

[27] *Best Practices for Conversions API*, META, https://www.facebook.com/business/help/308855623839366?id=%20818859032317965 (last visited Aug. 21, 2023).

implement the Tracking Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

78. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content on the host website. In other words, Facebook and others like it are not providing anything to the user related to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner.

79. Thus, without any knowledge, authorization, or action by the user, a website owner like Defendant can use its source code to commandeer its patients' computing devices, causing the devices' web browsers to contemporaneously and invisibly re-direct the patients' communications to hidden third parties.

80. In this case, Defendant employed just such a device to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to third parties like Facebook and Google contemporaneously, invisibly, and without the patient's knowledge.

81. Consequently, when Plaintiffs and Class Members visited Defendant's Online Platforms and communicated their Private Information, including but not limited to, medical treatment sought, medical conditions, appointment type and date, physician selected, specific button/menu selections, content (such as searches for symptoms or treatment options) typed into free text boxes, demographic information, email addresses, phone numbers, and emergency contact information, it is simultaneously intercepted and transmitted to third parties like Facebook and Google.

iii. Defendant Violated its own Privacy Policies

82. Defendant's Notice of Privacy Practices provides:

> Loyola Medicine is required by the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act (found in Title XIII of the American Recovery and Reinvestment Act of 2009) (collectively referred to as "HIPAA"), as amended from time to time, to maintain the privacy of individually identifiable patient health information (this information is "protected health information" and is referred to herein as "PHI"). We are also required to provide patients with a Notice of Privacy Practices regarding PHI. ***We will only use or disclose your PHI as permitted or required by applicable state law.*** This Notice applies to your PHI in our possession including the medical records generated by us.
>
> Loyola Medicine understands that your health information is highly personal, and we are committed to safeguarding your privacy. Please read this Notice of Privacy Practices thoroughly. It describes how we will use and disclose your PHI.[28]

83. Defendant's Notice of Privacy Practices does not permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes without written permission.[29]

84. Defendant violated its own Notice of Privacy Practices by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties.

85. The LUMC Notice of Privacy Practices states, "This Notice applies to the delivery of health care by Loyola Medicine and its medical staff in the main hospital, outpatient departments and clinics."[30]

86. The LUMC Notice of Privacy Practices further states:

> Subject to certain limited exceptions, your written authorization is required in cases where Loyola Medicine receives any direct or indirect financial remuneration in exchange for making the communication to you which encourages you to purchase

---

[28] *HIPAA Notice of Privacy Practices*, LOYOLA MEDICINE (Jan. 17, 2018), https://www.loyolamedicine.org/hipaa-notice-of-privacy-practices/ (emphasis added) (last visited Aug. 22, 2023).

[29] *Id.*

[30] *Id.*

a product or service or for a disclosure to a third party who wants to market their products or services to you.[31]

87. The LUMC Website Terms of Use and Online Privacy further represents as follows:

> Welcome to the website of LoyolaMedicine.org (the "Site"). This site is owned by Loyola University Health System ("Company"). Your compliance with these Terms of Use / Online Privacy ("Terms of Use") is a condition to your use of the site. If you do not agree to be bound by the Terms of Use, promptly exit this Site.
>
> Please consult the Online Privacy portion of these Terms of Use for information regarding our practices with respect to collection, use and sharing of personal information through this Site. Please consult our Notice of Privacy Practices for information on how we use patient information and your rights regarding your patient information.
>
> . . .
>
> **Online Privacy**
>
> **Scope.** This section describes how we use and share personal information collected through this Site. Our Site also contains links to third party sites that are not owned or controlled by Company. Please be aware that we are not responsible for the privacy practices of such other sites. We encourage you to be aware when you leave our Site and to read the privacy statements of each and every website that collects personal information. For information about how we collect, use and share your health and medical information, please refer to our Notice of Privacy Practices.
>
> **Information You Provide To Us.** You can provide information to us on our Site through various means, such as contacting us through our Site, filling out feedback forms, paying your hospital bills online or purchasing products online from our gift store. Depending on which feature you are using, you may be asked to provide personal information, such as name, address, telephone number, email address, credit or debit card information, bank account information and more.
>
> . . .
>
> **Information We Collect Automatically.** We collect certain information automatically as you use our Site, such as IP address, browser type, computer or device type, the website from where you navigated to our Site and the pages on our Site that you view.
>
> **Cookies.** When you visit our Site we send one or more "cookies" to your computer or other device. A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognize your browser. Cookies may store unique

[31] *Id.*

> identifiers, user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. We use cookies to improve the quality of our service, including for storing user preferences, tracking user trends and providing relevant advertising to you.
>
> **How We Use and Share Your Information**
>
> **Communications from Us.** We respect and are committed to protecting your privacy. We may collect personally identifiable information, including your email address, when you visit our Site. We also automatically receive and record information on our server logs from your browser including your IP address, cookie information and the page(s) you visited. We will use the information to contact you about products, services and information and to provide relevant advertising to you. ***We will not sell your personally identifiable information***, but we may provide your email address to third parties who will contact you about our products and services or whose products or services would be of interest to you.
>
> **To Provide Products, Services and Information.** We collect personal information from you so that we can provide products and services that you purchase using the Site and information that you request from us. We use your personal information to contact you about your orders, process credit card/debit card transactions and ship products to you. We may provide information to third party service providers that help us bring you the services we offer. For example, we use third parties to help host and maintain our Site and to process payments.[32]

88. Defendant violated its own Notice of Privacy Practices and Terms of Use and Online Privacy by unlawfully disclosing Plaintiffs' and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties. Defendant further misrepresented that it would preserve the confidentiality of their Private Information and the anonymity of their identities.

iv. Uncovering the Disclosure

89. In or around June 2022, The Markup, a nonprofit newsroom and media organization focusing on technology and its effects on society, conducted an investigation of the use of tracking

[32] *Terms of Use and Online Privacy*, LOYOLA MEDICINE (Aug. 16, 2012), https://www.loyolamedicine.org/terms-of-use-and-online-privacy/ (emphasis added) (last visited Aug. 22, 2023).

tools, such as the Tracking Pixel, on the online platforms of Newsweek's top 100 hospitals in America.[33]

90. The Markup discovered the Tracking Pixel was operating on 33 of the 100 hospitals investigated.[34] Defendant was one such hospital found operating the Pixel on its website—specifically, the webpage that allows patients to book appointments with healthcare providers.[35]

91. Following notification by The Markup of the risks the Pixel poses to the security of patients' Private Information, Defendant failed to remove the Pixel from its Online Platforms, including its appointment scheduling webpage.[36]

92. An example illustrates the point. If a user visits Defendant's Website and clicks on the "Find a Doctor" tab, the individual's browser sends a request to Defendant's server requesting that it load the webpage. Because LUMC utilizes the Tracking Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, causing the browser to secretly duplicate the communication with LUMC, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

93. For example, if the user clicks "Find a Doctor" and enters their Zip Code and the doctor's specialty, like "Addiction Psychiatry," this information is shared with Facebook, Google, or others that Defendant has configured its Pixels to interact with.

---

[33] Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (last visited Aug. 22, 2023).

[34] *Id.*

[35] *Id.*

[36] *Id.*

94. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

95. Every time LUMC sends a patient's website activity data to Facebook, that patient's PII is also disclosed, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to the corresponding Facebook profile and the person's real-world identity. A user who accesses LUMC's Online Platforms while logged into Facebook will transmit the user cookie to Facebook, which contains that user's unencrypted Facebook ID.

96. Google and other companies likewise process this data in a similar manner and use it to connect the information to particular individuals to build marketing and other data profiles.

97. Through the Pixel, Defendant shares its patients' identities and online activity, including personal information and search results related to their private medical treatment.

98. Defendant could have configured its tracking software to limit the information that it communicated to third parties, but it did not and instead intentionally selected the features and functionality of the Pixel that resulted in the Disclosure.

99. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information or assist with intercepting their communications. Plaintiffs were never provided with any written notice that Defendant discloses its patients' protected health information, nor were they provided any means of opting out of such disclosures. Defendant

nonetheless knowingly disclosed Plaintiffs' protected health information to Facebook, Google, and other unauthorized entities.

100. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on LUMC to keep their Private Information confidential and securely maintained, to use this information for legitimate healthcare purposes only, and to make only authorized disclosures of this information.

101. By law, Plaintiffs are entitled to privacy in their protected health information and confidential communications. LUMC deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiffs' and Class Members' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected information to Facebook and others—unauthorized third-party eavesdroppers; and (3) undertook this pattern of conduct without notifying Plaintiffs and Class Members and without obtaining their express written consent.

B. Plaintiffs' Experiences

i. Plaintiff Kensandra Smith's Experience

102. Plaintiff received healthcare services from one of the hospitals in LUMC's network and relied on LUMC's Online Platforms to communicate confidential patient information.

103. Plaintiff accessed Defendant's Online Platforms to receive healthcare services from Defendant at Defendant's direction and encouragement. Plaintiff reasonably expected that her online communications with LUMC were confidential, solely between herself and LUMC, and that such communications would not be transmitted to or intercepted by a third party.

104. Plaintiff is also a Facebook user and visited LUMC's Online Platforms while logged into Facebook.

105. Plaintiff used LUMC's Online Platforms to schedule an appointment for medical care, review her personal health information, and communicate her Private Information to LUMC. Plaintiff trusted that her Private Information would be safeguarded according to LUMC's privacy policies and state and federal law.

106. As described herein, LUMC sent Plaintiff's Private Information to Meta (Facebook), Google, and others when she used LUMC's digital platforms to communicate healthcare and identifying information to LUMC.

107. Pursuant to the process described herein, LUMC assisted Meta (Facebook), Google, and others with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Defendant facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

108. By failing to receive the requisite consent, LUMC breached confidentiality and unlawfully disclosed Plaintiff's personally identifiable information and protected health information.

109. Since Plaintiff began using LUMC's Online Platforms, Plaintiff has received targeted medical advertising on social media related to medical treatment. Specifically, Plaintiff Smith [redacted]

ii. Plaintiff Mary Ellen Nilles' Experience

110. Plaintiff received healthcare services from one of the hospitals in LUMC's network and relied on LUMC's Online Platforms to communicate confidential patient information.

111. Plaintiff accessed Defendant's Online Platforms to receive healthcare services from Defendant at Defendant's direction and encouragement. Plaintiff reasonably expected that her online communications with LUMC were confidential, solely between herself and LUMC, and that such communications would not be transmitted to or intercepted by a third party.

112. Plaintiff is also a Facebook user and visited LUMC's Online Platforms while logged into Facebook.

113. Plaintiff used LUMC's Online Platforms to schedule an appointment for medical care, review her personal health information, and communicate her Private Information to LUMC. Plaintiff trusted that her Private Information would be safeguarded according to LUMC's privacy policies and state and federal law.

114. As described herein, LUMC sent Plaintiff's Private Information to Meta (Facebook), Google, and others when she used LUMC's digital platforms to communicate healthcare and identifying information to LUMC.

115. Pursuant to the process described herein, LUMC assisted Meta (Facebook), Google, and others with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information, and related confidential information. Defendant facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

116. By failing to receive the requisite consent, LUMC breached confidentiality and unlawfully disclosed Plaintiff's personally identifiable information and protected health information.

117. Since Plaintiff began using LUMC's Online Platforms, Plaintiff has received targeted medical advertising on social media related to medical treatment. Specifically, Plaintiff Nilles used LUMC's Online Platforms in connection with seeking healthcare services [redacted].

C. Defendant Violated HIPAA Standards

118. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[37]

119. Guidance from the United States Department of Health and Human Services ("HHS") instructs healthcare providers that patient status alone is protected by HIPAA.

120. The HIPAA Privacy Rule, located at 45 CFR Part 160 and Subparts A and E of Part 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[38]

[37] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

[38] *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Aug. 22, 2023).

121. The Privacy Rule broadly defines "protected health information" ("PHI") as individually identifiable health information ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."[39]

122. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse;" (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."[40]

123. Under the HIPAA de-identification rule, "health information is not individually identifiable only if": (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination;" or (2)(i) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed: (A) Names; . . . (H) Medical record numbers; . . . (J) Account numbers; . . . (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; . . . and (R) [a]ny other unique identifying number, characteristic, or code . . . ; and (ii) [t]he covered entity must not have actual knowledge that the information could be used

[39] 45 C.F.R. § 160.103.

[40] *Id.*

alone or in combination with other information to identify an individual who is a subject of the information."[41]

124. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization.[42]

125. An individual or corporation violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-1320d-9 ("Part C"): "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[43] The statute states that a "person . . . shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization."[44]

126. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

127. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties.[45] There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use

[41] 45 C.F.R. § 160.514.

[42] *Id.* §§ 160.103, 164.502.

[43] 42 U.S.C. § 1320d-6.

[44] *Id.*

[45] *Id.*

individually identifiable health information for commercial advantage, personal gain, or malicious harm."[46] In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both."[47]

128. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, HHS instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data . . . . If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[48]

129. In its guidance for Marketing, HHS further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list.[49]

---

[46] *Id.*

[47] *Id.*

[48] OFFICE OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (2012), *available at* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

[49] OFFICE OF CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., MARKETING (2003), *available at* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Aug. 22, 2023).

130. HHS has repeatedly instructed for years that patient status is protected by the HIPAA Privacy Rule:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA.[50]

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list.[51]

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers."[52]

131. In addition, the Office for Civil Rights (OCR) at HHS has issued a Bulletin (the "HHS Bulletin") to highlight the obligations of HIPAA-covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies.[53]

132. The HHS Bulletin expressly provides,

> Tracking technologies are used to collect and analyze information about how users interact with regulated entities' websites or mobile applications ("apps"). For example, a regulated entity may engage a technology vendor to perform such analysis as part of the regulated entity's health care operations. The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures[54] of PHI to tracking technology vendors or any other violations of the HIPAA Rules. For example, disclosures of PHI to tracking technology**

[50] 65 Fed. Reg. 82717 (Dec. 28, 2000).

[51] 67 Fed. Reg. 53186 (Aug. 14, 2002).

[52] 78 Fed. Reg. 5642 (Jan. 25, 2013).

[53] *See Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, *supra* note 9.

[54] *See id.* at n.8 ("Regulated entities can use or disclose PHI, without an individual's written authorization, only as expressly permitted or required by the HIPAA Privacy Rule. *See* 45 CFR 164.502(a).").

> **vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.[55]**

133. Tracking technology vendors like Facebook and Google are considered business associates under HIPAA where, as here, they provide services to Defendant and receive and maintain PHI.

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[56]

134. The HHS Bulletin explained that, through tracking technologies such as the Tracking Pixel, covered entities disclose individual's information, including PHI, provided when individuals use the entity's website or mobile applications, such as medical records numbers, addresses, appointment dates, person's IP addresses or location, medical device IDs or unique identifying codes.[57]

135. The Bulletin further explained that "[a]ll such IIHI [individually identifiable health information] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI,

---

[55] *Id.* (citations omitted) (emphasis added) (citing 45 C.F.R. § 164.508(a)(3); 45 C.F.R. § 164.501 (defining "Marketing")).

[56] *Id.*

[57] *Id.*

such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services."[58] This is because that information "connects the individual to the regulated entity . . . and thus relates to the individual's past, present, or future health or health care or payment for care."[59]

136. HIPAA applies to Defendant's webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal **… [and pages] that address[] specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.[60]

137. Ultimately, in the Bulletin, HHS made clear that covered entities, such as LUMC, must comply with HIPAA rules in connection with tracking technologies such as the Tracking Pixel, including but not limited to:

- Ensuring that all disclosures of PHI to tracking technology vendors are specifically permitted by the Privacy Rule and that, unless an exception applies, only the minimum necessary PHI to achieve the intended purpose is disclosed.

---

[58] *Id*.

[59] *Id*.

[60] *Id.* (emphasis added).

- Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.

- If there is not an applicable Privacy Rule permission or if the vendor is not a business associated of the regulated entity, then the individuals' HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.

  Further, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.[61]

138. As articulated in the HHS Bulletin, covered entities utilizing tracking technologies must also implement "administrative, physical, and technical safeguards" to protect transmitted PHI, such as appropriate encryption, authentication, and audit controls; and must notify affected individuals and others of any impressible disclosure of PHI to tracking technology vendors who compromise that PHI. "In such instances, there is a presumption that there has been a breach of unsecured PHI unless the regulated entity can demonstrate that there is a low probability that the PHI has been compromised."[62]

139. The HHS Bulletin further noted that the impermissible disclosure of PHI can cause myriad harm to individuals, including "identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the

[61] *Id*. (internal citations omitted).

[62] *Id*.

individual or to others identified in the individual's PHI" and discloses highly sensitive information regarding patients' diagnoses, and the nature, frequency and location of treatment.[63]

140. The Bulletin is not a pronouncement of new law, but instead reminded covered entities and business associates of their longstanding obligations under existing guidance. The HHS Bulletin cautioned that, "[w]hile it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule."[64]

141. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Tracking Pixel.

D. Defendant Violated Industry Standards

142. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

143. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

144. AMA Code of Medical Ethics Opinion 3.1.1 provides:

> Protecting information gathered in association with the care of the patient is a core value in health care. . . . Patient privacy encompasses a number of aspects, including, . . . personal data (informational privacy).[65]

145. AMA Code of Medical Ethics Opinion 3.2.4 provides:

---

[63] *Id*.

[64] *Id*.

[65] *Opinion 3.1.1: Privacy in Health Care*, AM. MED. ASS'N, https://code-medical-ethics.ama-assn.org/ethics-opinions/privacy-health-care (last visited Sept. 13, 2023).

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified[, and] (b) [f]ully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted.[66]

146. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must: . . . (c) release patient information only in keeping ethics guidelines for confidentiality.[67]

E. Defendant Violated Standards Set Forth in Illinois Law

147. Under the Illinois Medical Patient Rights Act ("MPRA"), Plaintiffs and Class Members have rights to privacy and confidentiality in their health care.[68]

148. The MPRA provides:

> Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients, except that such information may be disclosed: (1) to the patient, (2) to the party making treatment decisions if the patient is incapable of making decisions regarding the health services provided, (3) for treatment in accordance with 45 CFR 164.501 and 164.506, (4) for payment in accordance with 45 CFR 164.501 and 164.506, (5) to those parties responsible for peer review, utilization review, and quality assurance, (6) for health care operations in accordance with 45 CFR 164.501 and 164.506, (7) to those parties required to be notified under the Abused and Neglected Child Reporting Act or the Illinois Sexually Transmissible Disease

---

[66] *Opinion 3.2.4: Access to Medical Records by Data Collection Companies*, AM. MED. ASS'N, https://code-medical-ethics.ama-assn.org/ethics-opinions/access-medical-records-data-collection-companies (last accessed Sept. 13, 2023).

[67] *Opinion 3.3.2: Confidentiality & Electronic Medical Records*, AM. MED. ASS'N, https://code-medical-ethics.ama-assn.org/ethics-opinions/confidentiality-electronic-medical-records (last visited Sept. 13, 2023).

[68] 410 ILL. COMP. STAT. 50/3(d).

> Control Act, or (8) as otherwise permitted, authorized, or required by State or federal law. This right may be waived in writing by the patient or the patient's guardian or legal representative, but a physician or other health care provider may not condition the provision of services on the patient's, guardian's, or legal representative's agreement to sign such a waiver.[69]

149. Furthermore, the Illinois Personal Information Protection Act ("IPIPA") protects Plaintiffs' and Class Members' Medical Information and Personal Information from unauthorized disclosure.[70]

150. LUMC is a "Data Collector" and subject to the provisions of the IPIPA.[71]

151. The IPIPA requires "data collectors" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."[72]

152. LUMC's disclosure of Plaintiffs' and Class Members' Private Information to third parties, including Meta (Facebook), Google, and likely others, through the operation of the Tracking Pixel on its Online Platforms violated Plaintiffs' and Class Members' rights to privacy and confidentiality in their receipt of healthcare services and fell below the applicable standard for safeguarding the confidential Private Information of Plaintiffs and Class Members.

F. Plaintiffs' and Class Members' Expectation of Privacy

153. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

---

[69] *Id.*

[70] 815 ILL. COMP. STAT. 530/5, /45.

[71] *See id.* at 530/5.

[72] *Id.* at 530/45.

154. Indeed, at all times when Plaintiffs and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

G. IP Addresses Are Personally Identifiable Information

155. On information and belief, through the use of the Tracking Pixels on Defendant's Online Platforms, Defendant also disclosed and otherwise assisted Facebook, Google, and/or other third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

156. An IP address is a number that identifies the address of a devise connected to the Internet.

157. IP addresses are used to identify and route communications on the Internet.

158. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

159. Facebook tracks every IP address ever associated with a Facebook user.

160. Facebook tracks IP addresses for use of targeting individual homes and their occupants with advertising.

161. Under HIPAA, an IP address is considered personally identifiable information:

- HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses.[73]

[73] *See* 45 C.F.R. § 164.514(2).

- HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information."[74]

162. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

H. Defendant Was Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures

163. The sole purpose of the use of the Tracking Pixel on Defendant's Online Platforms was marketing and profits.

164. In exchange for disclosing the Private Information of its patients, Defendant is compensated by third parties, like Facebook and Google, in the form of enhancing advertising services and more cost-efficient marketing on its platform.

165. Retargeting is a form of online marketing that targets users with ads based on their pervious internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients, including Plaintiffs and Class Members.

166. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

I. Plaintiffs' and Class Members' Private Information Had Financial Value

167. Plaintiffs' data and Private Information has economic value, and Defendant's disclosure harmed Plaintiffs and the Class. Facebook regularly uses data that it acquires to create

[74] 45 C.F.R. § 164.514(2)(ii); *see also* 45 C.F.R. § 164.514(b)(2)(i)(O).

Core and Custom Audiences, as well as Lookalike Audiences and then sells that information to advertising clients.

168. Data harvesting is one of the fastest growing industries in the country, and consumer data is so valuable that it has been described as the "new oil." Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

169. The value of health data in particular is well-known and has been reported on extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it describes the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[75]

170. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[76]

CLASS ACTION ALLEGATIONS

171. Plaintiffs bring this action pursuant to 735 ILCS 5/2-801 on behalf of themselves and all others similarly situated (the "Class") defined as:

> All citizens of Illinois whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel and related tracking technologies on Defendant's Online Platforms.

---

[75] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry*, TIME (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/ (last visited Aug. 22, 2023).

[76] Christina Farr, *Hospital Execs Say They are Getting Flooded with Requests for Your Health Data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Aug. 22, 2023).

172. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, was well as their immediate family members.

173. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

174. **Numerosity:** The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly accessed in the Disclosure, and each Class Member is apparently identifiable within Defendant's records.

175. **Commonality:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include, without limitation:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' Private Information;

b. Whether Defendant had duties not to disclose the Plaintiffs' and Class Members' Private Information to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for non-healthcare purposes;

d. Whether Defendant had duties not to use Plaintiffs' and Class Members' Private Information for unauthorized purposes;

e. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;

f. Whether and when Defendant actually learned of the Disclosure;

g. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

i. Whether Defendant failed to properly implement and configure the tracking software on its Online Platforms to prevent the disclosure of information compromised in the Disclosure;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Disclosure to occur; and

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting that it would safeguard Plaintiffs' and Class Members' Private Information.

176. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Disclosure, due to Defendant's use and incorporation of the tracking software.

177. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be

antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class, and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

178. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

179. **Predominance:** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

180. **Superiority and Manageability:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication or relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

181. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonable consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

182. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

183. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

184. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful disclosure and failure to properly secure the Private Information of Class Members, Defendant

may continue to refuse to provide proper notification to Class Members regarding the Disclosure, and Defendant may continue to act unlawfully as set forth in this Complaint.

185. Furthermore, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

186. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to the disclosure of patient information;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Disclosure;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Private Information; and

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

187. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

188. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, misused, and disclosed to unauthorized parties.

189. As a provider of health care under the law, Defendant had a special relationship with Plaintiffs and Class Members who entrusted Defendant to adequately protect their Private Information.

190. Defendant knew that the Private Information at issue was private and confidential and should be protected as private and confidential, and thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of unauthorized disclosure.

191. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and allowing it to be accessed by unauthorized third parties.

192. Defendant's failure to take proper security measures to protect Plaintiffs' and Class Members' Private Information created conditions conducive to a foreseeable risk of unauthorized access and disclosure of Private Information to unauthorized third parties. As described above, Plaintiffs and Class Members are part of a foreseeable, discernable group that was at high risk of having their Private Information compromised, and otherwise wrongly disclosed if not adequately protected by Defendant.

193. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

194. Defendant owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Private Information being improperly disclosed to unauthorized third parties.

195. Defendant systematically failed to provide adequate security for data in its possession or over which it had supervision and control.

196. Defendant, through its actions and omissions, unlawfully breached duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendant's possession, supervision, and control.

197. Defendant, through its actions and omissions, unlawfully breached duties owed to Plaintiffs and Class Members by failing to have appropriate procedures in place to prevent dissemination of Plaintiffs' and Class Members' Private Information.

198. Defendant, through its actions and omissions, unlawfully breached duties to timely and fully disclose to Plaintiffs and Class Members that the Private Information within Defendant's possession, supervision, and control was improperly accessed by unauthorized third parties, the nature of this access, and precisely the type of information improperly accessed.

199. Defendant's breach of duties owed to Plaintiffs and Class Members proximately caused Plaintiffs' and Class Members' Private Information to be compromised by being accessed by unauthorized third parties.

200. As a result, of Defendant's ongoing failure to adequately notify Plaintiffs and Class Members regarding what type of Private Information has been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages.

201. As a proximate result of Defendant's negligence and breach of duties as set forth above, Defendant's breaches of duty caused Plaintiffs and Class Members to, inter alia, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their Private Information, diminution in the value of their personal data for which there is a tangible value, and/or a loss of control over their Private Information, all of which can constitute actionable actual damages.

202. In failing to secure Plaintiffs' and Class Members' Private Information, Defendant is guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless, willful,

or conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, in addition to seeking actual damages, also seek punitive damages on behalf of themselves and the Class.

203. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' Private Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs and Class Members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

204. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

205. Plaintiffs allege this negligence *per se* theory as alternative to their other negligence claims.

206. Pursuant to the laws set forth herein, including 410 ILCS 50/3(d), 815 ILCS 530/5 *et seq*, the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Private Information.

207. Plaintiffs and Class Members are within the class of persons that these statutes and rules were designed to protect.

208. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' Private Information.

209. Defendant owed a duty to timely and adequately inform Plaintiffs and Class Members, in the event of their Private Information being improperly disclosed to unauthorized third parties.

210. It was not only reasonably foreseeable, but it was intended, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party such as Facebook gaining access to Plaintiffs' and Class Members' Private Information, resulting in Defendant's liability under principles of negligence per se.

211. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information and not complying with applicable industry standards as described in detail herein.

212. Plaintiffs' and Class Member's Private Information constitute personal property that was taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury and damages to Plaintiffs and Class Members.

213. As a proximate result of Defendant's negligence and breach of duties as set forth above, Defendant's breaches of duty caused Plaintiffs and Class Members to, inter alia, have their data shared with third parties without their authorization or consent, receive unwanted advertisements that reveal seeking treatment for specific medical conditions, fear, anxiety and worry about the status of their Private Information, diminution in the value of their personal data

for which there is a tangible value, and/or a loss of control over their Private Information, all of which can constitute actionable actual damages.

214. In failing to secure Plaintiffs' and Class Members' Private Information, Defendant is guilty of oppression, fraud, or malice. Defendant acted or failed to act with a reckless, willful, or conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs, in addition to seeking actual damages, also seek punitive damages on behalf of themselves and the Class.

215. Defendant's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class Members' Private Information, and as a result, Plaintiffs and Class Members have suffered and will continue to suffer damages as a result of Defendant's conduct. Plaintiffs and Class Members seek actual, compensatory, and punitive damages, and all other relief they may be entitled to as a proximate result of Defendant's negligence *per se.*

COUNT III
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

216. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

217. Plaintiffs' and Class Members' communications with Defendant constitute private conversations, communications, and information.

218. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Online Platforms.

219. Plaintiffs and Class Members communicated sensitive PHI and PII that they intended for only Defendant to receive and that they understood Defendant would keep private.

220. Plaintiffs and Class Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiffs' or Class Members' authorization, consent, or knowledge.

221. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations, Notice of Privacy Practices, and HIPAA. Moreover, Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

222. Defendant allowed the public disclosure of Plaintiffs' and Class Members' Private Information to Meta (Facebook), Google, and likely other third parties by allowing the Tracking Pixel and other tracking technologies to be used on its Online Platforms.

223. Defendant's actions gave publicity to the Private Information of Plaintiffs and Class Members.

224. Defendant's disclosure of PHI coupled with PII and the loss of privacy and confidentiality of Plaintiffs' and Class Members' Private Information is highly offensive to the reasonable person.

225. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiffs and Class Members is an intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion.

226. Plaintiffs and Class Members did not authorize, consent, know about, or take any action to indicate consent to Defendant's conduct alleged herein.

227. There is no legitimate public concern with respect to the Private Information of Plaintiffs and Class Members.

228. As a result of Defendant's public disclosure of Plaintiffs' and Class Members' Private Information, Plaintiffs and Class Members have been needlessly harmed by having their private and confidential medical information disseminated for profit by Defendant, Meta (Facebook), Google, and likely other third parties.

229. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

230. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

231. Plaintiffs and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiffs and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

COUNT IV
Breach of Implied Contract
(On Behalf of the Plaintiffs and the Class)

232. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

233. Defendant solicited and invited Plaintiffs and Class Members to provide their Private Information through Defendant's Online Platforms as part of its regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

234. Defendant required Plaintiffs and Class Members to provide their Private Information, including full names, email addresses, phone numbers, computer IP addresses, appointment information, medical insurance information, medical provider information, medical histories, and other content submitted on Defendant's Online Platforms as a condition of their receiving healthcare services.

235. As a condition of utilizing Defendant's Online Platforms and receiving services from Defendant, Plaintiffs and Class Members provided their Private Information and compensation for their medical care. In so doing, Plaintiffs and Class Members entered into contracts with Defendant by which Defendant agreed to safeguard and protect such information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

236. Implicit in the agreement between Defendant and its patients was the obligation that both parties would maintain the Private Information confidentially and securely.

237. Defendant had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class Members in its possession was used only as authorized, such as to provide medical treatment, billing, and other medical benefits from Defendant.

238. Defendant had an implied duty to protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses.

239. Additionally, Defendant implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

240. Plaintiffs and Class members reasonable believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

241. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information for uses other than medical treatment, billing, and benefits from Defendant.

242. Consumers of medical services value their privacy and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, nor would Plaintiffs and Class Members have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to monitor the Online Platforms, computer systems, and networks to ensure that reasonable data security measures were adopted and maintained.

243. Defendant breached the implied contracts with Plaintiffs and Class Members by disclosing Plaintiffs' and Class Members' Private Information to unauthorized third parties, failing to properly safeguard and protect Plaintiffs' and Class Members' Private Information; and violating industry standards as well as legal obligations that are necessarily incorporated into implied contract between Plaintiffs, Class Members, and Defendant.

244. The Disclosure was a reasonably foreseeable consequence of Defendant's actions in breach of the implied contracts.

245. Defendant's acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class Members to provide their Personal Information in exchange for medical treatment and benefits.

246. As a result of Defendant's failure to fulfill the data security protections promised in these implied contracts, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value.

247. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members have suffered (and will continue to suffer) the compromise and disclosure of their Private Information and identities, the loss of control of their Private Information, disruption of their medical care and treatment, and the loss of the benefit of the bargain they had struck with Defendant.

248. As a direct and proximate result of Defendant's above-described breach of contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

249. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

250. This claim is pleaded solely in the alternative to Plaintiffs' breach of implied contract claims.

251. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for

valuable services from third parties. Additionally, Plaintiffs and Class Members conferred a benefit on Defendant in the form of monetary compensation.

252. Plaintiffs and Class Members would not have used Defendant's services or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties.

253. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

254. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

255. The benefits that Defendant derived from Plaintiffs and Class Members rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

256. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds it received as a result of its conduct and the Disclosure alleged herein.

COUNT VI
Breach of Implied Duty of Confidentiality
(On Behalf of the Plaintiffs and the Class)

257. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

258. Plaintiffs and Class Members were patients of Defendant and received healthcare services from Defendant.

259. Defendant agreed to keep Plaintiffs' and Class Members' information confidential as part of establishing and maintaining the healthcare services provider/patient relationship between Defendant and Plaintiffs and Class Members.

260. There is a duty of confidentiality implied in every healthcare provider and patient relationship, akin to an implied contract, such that healthcare services providers may not disclose confidential information acquired through the healthcare provider-patient relationship.[77]

261. The implied duty of confidentiality is at least as extensive as Defendant's statutory obligations as a healthcare services provider to maintain patient confidentiality.

262. Under the Illinois Medical Patient Rights Act, "health care provider[s]" must "refrain from disclosing the nature or details of services provided to patients."[78]

263. Under 735 ILCS 5/8-802, "[n]o physician or surgeon shall be permitted to disclose any information he or she may have acquired in attending any patient in a professional character."

264. Defendant may also not disclose PII about a patient, potential patient, or household member of a patient for marketing purposes without the patient's express written authorization.[79]

265. Plaintiffs and Class Members performed all required conditions of their implied contracts with Defendant.

---

[77] *See e.g.*, *Geisberger v. Willuhn*, 72 Ill. App. 3d 435, 438 (2d Dist. 1979).

[78] 410 ILL. COMP. STAT. 50/3.

[79] *See* HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501, 164.508(a)(3), 164.514(b)(2)(i).

266. Defendant breached the implied duty of confidentiality to Plaintiffs and Class Members by intentionally deploying Tracking Pixels on its Online Platforms that caused the transmission of PII, PHI, and confidential communications to third parties, including Facebook.

267. Plaintiffs seek all monetary and non-monetary relief allowed by law.

COUNT VII
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. Comp. Stat. 505/1 *et seq.*
(On Behalf of Plaintiffs and the Class)

268. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

269. Defendant is a "person" as defined by 815 ILCS § 505/1.

270. Plaintiffs and the Class Members are "consumers" as defined by 815 ILCS § 505/1.

271. Defendant's unfair acts and practices against Plaintiffs and the Class Members occurred in the course of trade or commerce in Illinois, arose out of transactions that occurred in Illinois, and/or harmed individuals in Illinois.

272. Plaintiffs and the Class Members received and paid for health care services from Defendant.

273. Plaintiffs and the Class Members used Defendant's Online Platforms in connection with receiving health care services from Defendant.

274. Plaintiffs' and the Class Members' payments to Defendant for health care services were for household and personal purposes.

275. Defendant's practices of disclosing Plaintiffs' and the Class Members' PII and PHI by re-directing confidential communications via the Tracking Pixel to third parties without authorization, consent, or knowledge of Plaintiffs and the Class Members is a deceptive, unfair, and unlawful trade act or practice, in violation of 815 ILCS § 505/2.

276. Defendant's unfair business practices were targeted at all of Defendant's patients, including Plaintiffs and the Class Members.

277. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the privacy, security, and use of their personally identifiable patient data and communications when using Defendant's Online Platforms.

278. Defendant intended to mislead Plaintiffs and the Class Members and to induce them to rely on its misrepresentations and omissions.

279. Defendant's surreptitious collection and disclosure of Plaintiffs' and the Class Members' PII, PHI, and communications to third parties involves important consumer protection concerns.

280. Furthermore, the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/20, provides that a violation of that statute constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 *et seq.* ("ICFA").

281. Defendant is a "data collector" under IPIPA.[80] As a data collector, Defendant owns or licenses information concerning Illinois residents.

282. IPIPA protects Medical Information and Personal Information.[81]

283. The IPIPA requires a data collector that "maintains or stores . . . records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."[82]

---

[80] 815 ILL. COMP. STAT. 530/5.

[81] *Id.*

[82] 815 ILL. COMP. STAT. 530/45(a).

284. IPIPA's rights are not subject to waiver.[83]

285. Defendant represented that it would safeguard and protect Plaintiffs' and Class Members' Private Information, in its Privacy Practices and elsewhere, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

286. Defendant made these representations with the intent to induce Plaintiffs and Class Members to seek health care services from Defendant and to use Defendant's Online Platforms in doing so.

287. Plaintiffs and Class Members relied upon Defendant's representations in seeking health care services from Defendant and in using Defendant's Online Platforms to obtain such services.

288. The IPIPA further requires that data collectors "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most *expedient* time possible and *without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system."[84]

289. As alleged above, Defendant violated the IPIPA by failing to implement and maintain reasonable security measures to protect Plaintiffs and Class Members' PHI and PII. Defendant further violated the IPIPA by failing to give Plaintiffs and Class Members expedient notice without unreasonable delay.

[83] 815 ILL. COMP. STAT. 530/15.

[84] 815 ILL. COMP. STAT. 530/10 (emphasis added).

290. As a direct and proximate cause of Defendant's unfair acts and practices, Plaintiffs and Class members have suffered actual damages.

291. Plaintiffs' and the Class Members' injuries were proximately caused by Defendant's unfair and deceptive business practices.

292. As a result of Defendant's conduct, Defendant has been unjustly enriched.

293. Defendant's acts caused substantial injury that Plaintiffs and the Class Members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

294. Defendant acted intentionally, knowingly, and maliciously to violation Illinois's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiffs' and the Class Members' rights.

295. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including overpaying for Defendant's health care services and loss of value of their personally identifiable patient data and communications.

296. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Plaintiffs and the Class Members were also damaged by Defendant's conduct in that:

a. Defendant harmed Plaintiffs' and Class Members' interest in privacy;

b. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private has been disclosed to third parties;

c. Defendant eroded the essential confidential nature of the provider-patient relationship;

d. Defendant took something of value from Plaintiffs and Class Members, i.e., their personally identifiable patient information, and derived a benefit therefrom without Plaintiffs' or the Class Members' authorization, informed consent, or knowledge, and without sharing the benefit of such value;

e. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

f. Defendant's actions diminished the value of Plaintiffs' and Class Members' personal information.

297. As a direct and proximate result of Defendant's above-described violation of the IPIPA and ICFA, Plaintiffs and Class Members are entitled to recover actual damages, reasonable attorneys' fees, and costs.

COUNT VIII
Violation of Illinois Eavesdropping Statute
720 Ill. Comp. Stat. 5/14 *et seq.*
(On Behalf of Plaintiffs and the Class)

298. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

299. The Eavesdropping Article of the Illinois Criminal Code (the "Illinois Eavesdropping Statute" or "IES") states that it is a felony for any person to knowingly and intentionally "use[] an eavesdropping devise, in a surreptitious manner, for the purpose of

transmitting or recording all or part of any private conversation to which he or she is a party unless he or she does so with the consent of all other parties to the private conversation."[85]

300. The IES also states that it is a felony for any person to knowingly and intentionally "use[] or disclose[] any information which he or she knows or reasonably should know was obtained from a private conversation or private electronic communication in violation of this Article, unless he or she does so with the consent of all of the parties."[86]

301. For purposes of the IES, "eavesdropping device" means "any device capable of being used to hear or record oral conversation or intercept, or transcribe electronic communications whether such conversation or electronic communication is conducted in person, by telephone, or by any other means."[87]

302. For purposes of the IES, "surreptitious" means "obtained or made by stealth or deception, or executed through secrecy or concealment."[88]

303. For purposes of the IES, "private electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation. . . . Electronic communication does include any communication from a tracking device."[89]

---

[85] 720 ILL. COMP. STAT. 5/14-2(a), -4.

[86] *Id.*

[87] 720 ILL. COMP. STAT. 5/14-1(a).

[88] 720 ILL. COMP. STAT. 5/14-1(g).

[89] 720 ILL. COMP. STAT. 5/14-1(e).

304. "A reasonable expectation shall include any expectation recognized by law, including, but not limited to, an expectation derived from a privilege, immunity, or right established by common law, Supreme Court rule, or the Illinois or United States Constitution."[90]

305. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' private electronic communications, without the consent of Plaintiffs and Class Members, using the Tracking Pixel and similar tracking technologies on its Online Platforms.

306. Defendant intentionally recorded and/or acquired Plaintiffs' and Class Members' private electronic communications for the purpose of disclosing those communications to third parties, including Facebook and Google, without the knowledge, consent, or written authorization of Plaintiffs or Class Members.

307. Plaintiffs' and Class Members' communications with Defendant constitute private conversations, communications, and information.

308. Plaintiffs and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Online Platforms.

309. Plaintiffs and Class Members communicated sensitive PHI and PII that they intended for only Defendant to receive and that they understood Defendant would keep private.

310. Plaintiffs and Class Members have a reasonable expectation that Defendant would not disclose PII, PHI, and confidential communications to third parties without Plaintiffs' or Class Members' authorization, consent, or knowledge.

311. Plaintiffs and Class Members had a reasonable expectation of privacy given Defendant's representations, Notice of Privacy Practices, Terms of Use, and HIPAA. Moreover,

[90] *Id.*

Plaintiffs and Class Members have a general expectation that their communications regarding healthcare with their healthcare providers will be kept confidential.

312. Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously recorded and transmitted to third parties as they communicated with Defendant through its Online Platforms.

313. Without Plaintiffs' or Class Members' knowledge, authorization, or consent, Defendant used the Tracking Pixel imbedded and concealed into the source code of its Online Platforms to secretly record and transmit Plaintiffs' and Class Members' private communications to hidden third parties, such as Facebook and Google.

314. Under the IES, "[a]ny or all parties to any conversation or electronic communication upon which eavesdropping is practices contrary to this Article shall be entitled to the following remedies: (a) [t]o an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either; (b) [t]o all actual damages against the eavesdropper or his principal or both; [t]o any punitive damages which may be awarded by the court or by a jury. . . ."[91]

315. The eavesdropping devices used in this case include, but are not limited to:

a. Plaintiffs' and Class Members' personal computing devices;

b. Plaintiffs' and Class Members' web browsers;

c. Plaintiffs' and Class Members' browser-managed files;

d. Facebook's Pixel;

e. Internet cookies;

f. Defendant's computing servers;

[91] 720 ILL. COMP. STAT. 5/14-6.

g. Third-party source code utilized by Defendant; and

h. Computer servers of third-parties (including Facebook) to which Plaintiffs' and Class Members' communications were disclosed.

316. The eavesdropping devices outlined above are not excluded "tracking devices" as that term is used in the IES, 720 ILCS 5/14-1(e), to the extent that they perform functions other than collection of geo-locational data.[92]

317. Defendant is a "person" under the IES.[93]

318. Defendant aided in the interception of communications between Plaintiffs and Class Members and Defendant that were redirected to and recorded by third parties without Plaintiffs' or Class Members' consent.

319. Under the IES, Plaintiffs and the Class Members are entitled to injunctive relief prohibiting further eavesdropping by Defendant, actual damages, and punitive damages.

320. Defendant's breach caused Plaintiffs and Class Members the following damages:

a. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the physician-patient relationship;

c. Defendant took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;

[92] *See Vasil v. Kiip, Inc.*, No. 16-cv-9937, 2018 U.S. Dist. LEXIS 35573, at *20-25 (N.D. Ill. Mar. 5, 2018).

[93] 720 ILL. COMP. STAT. 5/2-15.

d. Plaintiffs and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and

e. Defendant's actions diminished the value of Plaintiffs' and Class Members' personal information.

321. Plaintiffs and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Disclosure;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages under the IES and any other applicable law;

h) For an award of attorneys' fees and costs under the ICFA, the common fund doctrine, and any other applicable law;

i) Costs and any other expense, including expert witness fees incurred by Plaintiffs in connection with this action;

j) Pre- and post-judgment interest on any amounts awarded; and,

k) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs, pursuant to 735 ILCS 5/2-1105, hereby demand a trial by jury on all issues so triable.

Dated: September 26, 2023

Respectfully Submitted,

/s/ David S. Almeida
David S. Almeida

David S. Almeida (ARDC 6285557)
Elena A. Belov*
ALMEIDA LAW GROUP LLC
Firm ID 100530
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Tyler B. Ewigleben*
Christopher D. Jennings*
Winston Hudson*
Laura Edmondson*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
tyler@yourattorney.com
winston@yourattorney.com
ledmondson@yourattorney.com

*To be admitted *pro hac vice*
Counsel for Plaintiffs and the Proposed Class